

RECEIVED
CENTRAL FAX CENTER

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE OCT 11 2005

Application Serial No.09/651,424
Filing Date August 30, 2000
InventorMariusz H. Jakubowski et al.
Group Art Unit2134
Examiner Tran, Tongoc
Attorney's Docket No. MS1-528US
Confirmation No.2561
Title: Method and System for Using a Portion of a Digital Good as a Substitution
Box

APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Allan Sponseller (Tel. 509-324-9256x215; Fax 509-323-8979)
Customer No. 22801

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits an appeal brief for application 09/651,424, filed August 30, 2000, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

10/14/2005 BABRAHA1 00000009 120769 09651424

01 FC:1402 500.00 DA

<u>Appeal Brief Items</u>	<u>Page</u>
(1) Real Party in Interest	3
(2) Related Appeals and Interferences	3
(3) Status of Claims	3
(4) Status of Amendments	3
(5) Summary of Claimed Subject Matter	4
(6) Grounds of Rejection to be Reviewed on Appeal	6
(7) Argument	6
(8) Appendix of Appealed Claims	25
(9) Appendix of Evidence Submitted	32
(10) Appendix of Related Proceedings	33

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 1-9 and 11-36 stand rejected and are pending in this Application. Claims 1-9 and 11-36 are appealed. Claim 8 was previously amended. Claim 10 was previously canceled. Claims 1-9 and 11-36 are set forth in the Appendix of Appealed Claims on page 25.

(4) Status of Amendments

A Final Office Action was issued on January 12, 2005.

A Response to the Final Office Action was filed May 27, 2005. No amendments were made as part of this Response.

No Advisory Action has been received by Appellant.

Appellant filed a Notice of Appeal on July 11, 2005 in response to the Final Office Action.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters. These specific reference characters are examples of particular elements of the drawings for certain embodiments of the claimed invention, and the claims are not limited to solely the elements corresponding to these reference characters.

With respect to independent claim 1, as discussed for example at page 24, line 10 through page 26, line 12, one or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including selecting a portion of a digital good (902), selecting another portion of the digital good, wherein the other portion is to be encrypted (906), and using the portion as a substitution box (S-box) when encrypting the other portion (904, 908).

With respect to independent claim 8, as discussed for example at page 24, line 10 through page 26, line 12, a method comprises selecting a segment of a digital good (902) and selecting another segment of the digital good, wherein the other segment is to be encrypted using an encryption process (906). The method further comprises mapping, as at least part of the encryption process, values within the other segment to new values based on the segment, wherein the mapping comprises using the segment as a substitution box (S-box) during the encryption process (904, 908).

With respect to independent claim 17, as discussed for example at page 24, line 10 through page 26, line 12, a method comprises using at least a portion of a digital good as a substitution box (S-box) (904).

With respect to independent claim 25, as discussed for example at page 24, line 10 through page 26, line 12, a production system comprises a memory (120) to store an original program, and a production server (130). The production server (130) is equipped with a substitution box (S-box) protection tool (136(6)) that is used to augment the original program for protection purposes, the production server (130) being configured to identify a first segment in the original program and use the first segment as an S-box when encrypting a second segment of the original program.

With respect to independent claim 31, as discussed for example at page 24, line 10 through page 26, line 12, a client-server system, comprises a production server (130) and a client (104). The production server (130) is to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good. The client (104) is to store and execute the protected digital good, the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with.

With respect to independent claim 33, as discussed for example at page 24, line 10 through page 26, line 12, one or more computer readable media (142) having stored thereon a plurality of instructions that, when executed by one or more processors (140), causes the one or more processors (140) to perform acts including decrypting at least a portion of a digital good (124) by using another portion of the digital good (124) as a substitution box (S-box).

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-6, 8-9, 11-13, and 15-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 6,594,761 to Chow.

Claims 31-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 5,809,144 to Sirbu.

Claims 7 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 6,594,761 to Chow and further in view of U.S. Patent No. 5,809,144 to Sirbu.

(7) Argument

A. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 6,594,761 to Chow.

Claims 1-6, 8-9, 11-13, and 15-30 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle (hereinafter "Merkle") in view of U.S. Patent No. 6,594,761 to Chow (hereinafter "Chow").

Merkle is directed to method and apparatus for data encryption (see, Title). As discussed with reference to Figures 1 and 2 of Merkle, as well as the Abstract, the method uses part of the data input to access a table of pseudo-random numbers. The pseudo-random numbers are exclusively ORed (XORed) with the remaining part of the data input. The output from the XOR operation is then used to access the table where the other portion of the data is in turn XORed with the

pseudo random numbers. This iterative process continues until the data is fully randomized.

Chow is directed to tamper resistant software encoding (see, Title). As discussed in the Abstract of Chow, the method of the invention is to increase the tamper-resistance and obscurity of computer software code by transforming the data flow of the computer software so that the observable operation is dissociated from the intent of the original software code. A number of techniques for performing the invention are given, including encoding software arguments using polynomials, prime number residues, converting variables to new sets of Boolean variables, and defining variables on a new n-dimensional vector space.

1. Claims 1-6

With respect to claim 1, claim 1 recites:

One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

- selecting a portion of a digital good;
- selecting another portion of the digital good, wherein the other portion is to be encrypted; and
- using the portion as a substitution box (S-box) when encrypting the other portion.

Appellant respectfully submits that Merkle in view of Chow does not disclose or suggest selecting a portion of a digital good and using the portion as a substitution box as recited in claim 1.

In the May 5, 2004 Office Action at pages 2-3, Merkle at Fig. 1 and col. 2, line 51 – col. 3, line 21 is cited as teaching this selecting and using of claim 1. Appellant respectfully disagrees. The cited portions of Merkle discuss that data is

processed in 64-bit clear text blocks (see, col. 2, line 53). The initial 64-bit clear text block is split in half, creating an initial left half L_1 of 32 bits and an initial right half R_1 of 32 bits (see, col. 2, lines 53-56). These values are XORed with a 32-bit Auxiliary key 0 and 32 bit Auxiliary Key 1, and the output from this operation is an initial left half L_0 and an initial right half R_0 , each 32 bits in length (see, col. 2, lines 56-63). The rightmost eight bits of L_0 are used as an input to an S-box (see, emphasis added, col. 2, lines 64-66). The output from the S-box is a 32 bit entry which is then XORed with R_0 (see, col. 2, lines 66-67). L_0 is then rotated according to a predefined rotation schedule, and after its rotation the 32-bit word is labeled R_1 and used as the right half input in the next iteration of the encryption method (see, col. 2, line 67 – col. 3, line 3). The output from the XOR operation of R_0 and the S-box entry is labeled L_1 and used as the left half input in the next iteration of the encryption method (see, col. 3, lines 3-6).

Thus, the cited portions of Merkle discuss portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in the cited portions of Merkle, or elsewhere in Merkle, is there any discussion or even mention of using the 64-bit clear text block itself as the S-box.

In the January 12, 2005 Final Office Action at ¶ 2, p. 2, it was stated that:

Applicant's arguments filed 8/10/2004 have been fully considered but they are not persuasive. Applicant contends that the cited prior art, Merkle (U.S. Patent No. 5,003,597), "discuss portions of a 64 bit clear text block being used to calculate an input to a S-box, not being used as the S-box itself". Examiner respectfully disagrees. Merkle teaches the first portion of the clear text is selected as an input to a S-box (or can be interpreted as generate S-box based on values in first portion) (e.g. Fig. 1 and col. 2, line 64-col. 3, line 6).

Thus, it appears that the position taken in the January 12, 2005 Final Office Action is that in discussing an input to an S-box, Merkle is somehow disclosing using that input to generate the S-box. Appellant respectfully submits that an input to a thing and the thing itself are different – calculating the input to the thing does not describe calculating the thing itself. The input to the S-box may be used to generate the output of the S-box, but not to generate the S-box itself.

Appellant notes that Merkle does go on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key, satisfying a property that all four of the one-byte (8-bit) columns in the S-box must be permutations of one another (see, col. 4, lines 46-54). The pre-computation of a pseudo-random S-box satisfying the desired properties can be divided into two stages: first, a stream of pseudo-random bytes is generated; second, the stream of pseudo-random bytes is used to generate four pseudo-random permutations that map 8 bits to 8 bits (see, col. 5, lines 1-6). These four pseudo-random permutations are the generated S-box (see, col. 5, lines 6-7). However, such discussions of computation of an S-box make no mention whatsoever of selecting a portion of a digital good and using the portion as a substitution box.

As there is no discussion or even mention in Merkle of selecting a portion of a digital good and using that portion as an S-box when encrypting another portion as recited in claim 1, Appellant respectfully submits that Merkle cannot disclose or suggest the selecting and using of claim 1.

With respect to Chow, Chow is cited for “using DES technique to obfuscate digital good for tamper resistant protection”. Appellant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 1 is allowable over Merkle in view of Chow.

With respect to claims 2-6, given that claims 2-6 depend from claim 1, Appellant respectfully submits that claims 2-6 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 1.

2. Claims 8, 9, 11-13, and 15-16

With respect to claim 8, claim 8 recites:

A method comprising:
selecting a segment of a digital good;
selecting another segment of the digital good, wherein the other segment is to be encrypted using an encryption process; and
mapping, as at least part of the encryption process, values within the other segment to new values based on the segment, wherein the mapping comprises using the segment as a substitution box (S-box) during the encryption process.

Appellant respectfully submits that Merkle in view of Chow does not disclose or suggest the selecting and mapping as recited in claim 8.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of selecting a segment of a digital good and using the segment as a substitution box during an encryption process.

Without any discussion or mention of selecting a segment of a digital good and using the segment as a substitution box during an encryption process, Appellant respectfully submits that Merkle cannot disclose or suggest selecting a segment of a digital good, and mapping, as at least part of the encryption process, values within the other segment to new values based on the segment, wherein the mapping comprises using the segment as a substitution box (S-box) during the encryption process as recited in claim 8.

With respect to Chow, Chow is cited for "using DES technique to obfuscate digital good for tamper resistant protection". Appellant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 8 is allowable over Merkle in view of Chow.

With respect to claims 9, 11-13, and 15-16, given that claims 9, 11-13, and 15-16 depend from claim 8, Appellant respectfully submits that claims 9, 11-13, and 15-16 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 8.

3. Claims 17 and 21-24

With respect to claim 17, claim 17 recites:

A method comprising:
using at least a portion of a digital good as a substitution box
(S-box).

Appellant respectfully submits that Merkle in view of Chow does not disclose or suggest the using as recited in claim 17.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of using a portion of a digital good as an S-box.

Without any discussion or mention of using a portion of a digital good as an S-box, Appellant respectfully submits that Merkle cannot disclose or suggest using at least a portion of a digital good as a substitution box (S-box) as recited in claim 17.

With respect to Chow, Chow is cited for "using DES technique to obfuscate digital good for tamper resistant protection". Appellant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 17 is allowable over Merkle in view of Chow.

With respect to claims 21-24, given that claims 21-24 depend from claim 17, Appellant respectfully submits that claims 21-24 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 17.

4. Claims 18-20

With respect to claim 18, claim 18 depends from claim 17 and Applicant respectfully submits that claim 18 is allowable over Merkle in view of Chow at least because of its dependency on claim 17.

Furthermore, claim 18 recites:

A method as recited in claim 17, wherein the using comprises using the portion of the digital good as a substitution box to encrypt another portion of the digital good.

Appellant respectfully submits that Merkle in view of Chow does not disclose or suggest the using as recited in claim 18.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of using a portion of a digital good as a substitution box to encrypt another portion of the digital good.

Without any discussion or mention of using a portion of a digital good as a substitution box to encrypt another portion of the digital good, Appellant respectfully submits that Merkle cannot disclose or suggest using the portion of the digital good as a substitution box to encrypt another portion of the digital good as recited in claim 18.

With respect to Chow, Chow is cited for “using DES technique to obfuscate digital good for tamper resistant protection”. Appellant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 18 is allowable over Merkle in view of Chow.

With respect to claims 19 and 20, given that claims 19 and 20 depend from claim 18, Appellant respectfully submits that claims 19 and 20 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 18.

5. Claims 25-30

With respect to claim 25, claim 25 recites:

A production system, comprising:
a memory to store an original program; and
a production server equipped with a substitution box (S-box) protection tool that is used to augment the original program for protection purposes, the production server being configured to identify a first segment in the original program and use the first segment as an S-box when encrypting a second segment of the original program.

Appellant respectfully submits that Merkle in view of Chow does not disclose or suggest the production system as recited in claim 25.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random

fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of identification of a first segment in an original program and use of the first segment as an S-box when encrypting a second segment of the original program.

Without any discussion or mention of identification of a first segment in an original program and use of the first segment as an S-box when encrypting a second segment of the original program, Appellant respectfully submits that Merkle cannot disclose or suggest a production server equipped with a substitution box (S-box) protection tool that is used to augment the original program for protection purposes, the production server being configured to identify a first segment in the original program and use the first segment as an S-box when encrypting a second segment of the original program as recited in claim 25.

With respect to Chow, Chow is cited for "using DES technique to obfuscate digital good for tamper resistant protection". Appellant respectfully submits that Chow is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 25 is allowable over Merkle in view of Chow.

With respect to claims 26-30, given that claims 26-30 depend from claim 25, Appellant respectfully submits that claims 26-30 are likewise allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 25.

B. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 5,809,144 to Sirbu.

Claims 31-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle (hereinafter "Merkle") in view of U.S. Patent No. 5,809,144 to Sirbu (hereinafter "Sirbu").

Merkle is directed to method and apparatus for data encryption (see, Title). As discussed with reference to Figures 1 and 2 of Merkle, as well as the Abstract, the method uses part of the data input to access a table of pseudo-random numbers. The pseudo-random numbers are exclusively ORed (XORed) with the remaining part of the data input. The output from the XOR operation is then used to access the table where the other portion of the data is in turn XORed with the pseudo random numbers. This iterative process continues until the data is fully randomized.

Sirbu is directed to a method and apparatus for purchasing and delivering digital goods over a network (see, Title). As discussed in the Abstract of Sirbu, the method includes identifying a digital good to be purchased. A purchase price for the digital good is negotiated. After the negotiation step, an authenticated purchase request is sent to the merchant. The merchant encrypts the desired digital good and calculates a first cryptographic checksum for the encrypted good. The encrypted digital good and the first cryptographic checksum together with a timestamp are then transmitted to the customer. The customer calculates a second cryptographic checksum for the received encrypted digital good. The customer creates an electronic payment order containing information identifying the transaction, the second cryptographic checksum, credentials, and the timestamp.

The electronic payment order is transmitted to the merchant. The merchant compares the first and second cryptographic checksums to ensure that they match, and if so, the merchant adds an electronic signature and a decryption key to the electronic payment order. The merchant submits the merchant signed electronic payment order and the key to an account server for review. The account server reviews the information in the electronic payment order and sends a message, including the key if the review is positive, to the merchant. The merchant forwards the message to the customer. If the message contained the key, the customer uses the key to decrypt the goods.

1. Claim 31

With respect to claim 31, claim 31 recites:

A client-server system, comprising:
a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good; and
a client to store and execute the protected digital good, the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with.

Appellant respectfully submits that Merkle in view of Sirbu does not disclose or suggest a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good as recited in claim 1.

Merkle at col. 2, line 52-col. 3, line 35 is cited as teaching "Selecting portion of clear text as a substitution box (S-box) in encrypting at least a portion of a second portion of clear text to produce encrypted text". However, as discussed

above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of use of a portion of a first digital good as an S-box in encrypting at least a portion of a second digital good .

With respect to Sirbu, Sirbu is cited as teaching "a server production encrypts digital good; and a client to store and execute the protected digital good, the client being configure to evaluate the protected digital to determine whether the protected digital good has been tampered with". Appellant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 31 is allowable over Merkle in view of Sirbu.

2. Claim 32

With respect to claim 32, claim 32 depends from claim 31 and Applicant respectfully submits that claim 32 is allowable over Merkle in view of Sirbu at least because of its dependency on claim 31.

Furthermore, claim 32 recites:

A client-server system as recited in claim 31, wherein the first digital good and the second digital good are the same digital good.

Appellant respectfully submits that Merkle in view of Sirbu does not disclose or suggest a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good, wherein the first digital good and the second digital good are the same digital good as recited in claim 32.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of use of a portion of a digital good as an S-box in encrypting at least a portion of the digital good .

Without any discussion or mention of use of a portion of a digital good as an S-box in encrypting at least a portion of the digital good, Appellant respectfully submits that Merkle cannot disclose or suggest a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good, wherein the first digital good and the second digital good are the same digital good as recited in claim 32.

With respect to Sirbu, Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 32 is allowable over Merkle in view of Sirbu .

3. Claims 33-36

With respect to claim 33, claim 33 recites:

One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

decrypting at least a portion of a digital good by using another portion of the digital good as a substitution box (S-box).

Appellant respectfully submits that Merkle in view of Sirbu does not disclose or suggest decrypting at least a portion of a digital good by using another portion of the digital good as a substitution box (S-box) as recited in claim 33.

As discussed above, Merkle discusses portions of a 64-bit clear text block being used to calculate an input to an S-box, not being used as the S-box itself. Nowhere in Merkle is there any discussion or even mention of using the 64-bit clear text block itself as the S-box. Also as discussed above, Merkle goes on to discuss computation of an S-box by pre-computing an S-box in a pseudo-random fashion from a user supplied key. However, such discussions of computation of an S-box make no mention whatsoever of decrypting at least a portion of a digital good by using another portion of the digital good as an S-box.

Without any discussion or mention of decrypting at least a portion of a digital good by using another portion of the digital good as an S-box, Appellant respectfully submits that Merkle cannot disclose or suggest decrypting at least a portion of a digital good by using another portion of the digital good as a substitution box (S-box) as recited in claim 33.

With respect to Sirbu, Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle.

For at least these reasons, Appellant respectfully submits that claim 33 is allowable over Merkle in view of Sirbu.

With respect to claims 34-36, given that claims 34-36 depend from claim 33, Appellant respectfully submits that claims 34-36 are likewise allowable over Merkle in view of Sirbu for at least the reasons discussed above with respect to claim 33.

C. Rejection under 35 U.S.C. §103(a) over U.S. Patent No. 5,003,597 to Merkle in view of U.S. Patent No. 6,594,761 to Chow and further in view of U.S. Patent No. 5,809,144 to Sirbu.

Claims 7 and 14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,003,597 to Merkle (hereinafter "Merkle") in view of U.S. Patent No. 6,594,761 to Chow (hereinafter "Chow") and further in view of U.S. Patent No. 5,809,144 to Sirbu (hereinafter "Sirbu").

Merkle is directed to method and apparatus for data encryption (see, Title). As discussed with reference to Figures 1 and 2 of Merkle, as well as the Abstract, the method uses part of the data input to access a table of pseudo-random numbers. The pseudo-random numbers are exclusively ORed (XORed) with the remaining part of the data input. The output from the XOR operation is then used to access the table where the other portion of the data is in turn XORed with the pseudo random numbers. This iterative process continues until the data is fully randomized.

Chow is directed to tamper resistant software encoding (see, Title). As discussed in the Abstract of Chow, the method of the invention is to increase the tamper-resistance and obscurity of computer software code by transforming the data flow of the computer software so that the observable operation is dissociated from the intent of the original software code. A number of techniques for performing the invention are given, including encoding software arguments using polynomials, prime number residues, converting variables to new sets of Boolean variables, and defining variables on a new n-dimensional vector space.

Sirbu is directed to a method and apparatus for purchasing and delivering digital goods over a network (see, Title). As discussed in the Abstract of Sirbu, the method includes identifying a digital good to be purchased. A purchase price for the digital good is negotiated. After the negotiation step, an authenticated purchase request is sent to the merchant. The merchant encrypts the desired digital good and calculates a first cryptographic checksum for the encrypted good. The encrypted digital good and the first cryptographic checksum together with a timestamp are then transmitted to the customer. The customer calculates a second cryptographic checksum for the received encrypted digital good. The customer creates an electronic payment order containing information identifying the transaction, the second cryptographic checksum, credentials, and the timestamp. The electronic payment order is transmitted to the merchant. The merchant compares the first and second cryptographic checksums to ensure that they match, and if so, the merchant adds an electronic signature and a decryption key to the electronic payment order. The merchant submits the merchant signed electronic payment order and the key to an account server for review. The account server

reviews the information in the electronic payment order and sends a message, including the key if the review is positive, to the merchant. The merchant forwards the message to the customer. If the message contained the key, the customer uses the key to decrypt the goods.

1. Claim 7

With respect to claim 7, claim 7 depends from claim 1 and Appellant respectfully submits that claim 7 is allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 1. Appellant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle in view of Chow. For at least these reasons, Appellant respectfully submits that claim 7 is allowable over Merkle in view of Chow and further in view of Sirbu.

2. Claim 14

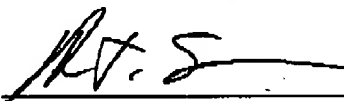
With respect to claim 14, claim 14 depends from claim 8 and Appellant respectfully submits that claim 14 is allowable over Merkle in view of Chow for at least the reasons discussed above with respect to claim 8. Appellant respectfully submits that Sirbu is not cited as curing, and does not cure, these deficiencies of Merkle in view of Chow. For at least these reasons, Appellant respectfully submits that claim 14 is allowable over Merkle in view of Chow and further in view of Sirbu.

Conclusion

The Office's basis and supporting rationale for the § 103(a) rejections is not supported by the teaching of the cited references. Appellant respectfully requests that the rejections be overturned and that pending claims 1-9 and 11-36 be allowed to issue.

Respectfully Submitted,

Dated: 10/11/05

By: 

Allan T. Sponseller
Lee & Hayes, PLLC
Reg. No. 38,318
(509) 324-9256 ext. 215

(8) Appendix of Appealed Claims

1. (Original) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

selecting a portion of a digital good;

selecting another portion of the digital good, wherein the other portion is to be encrypted; and

using the portion as a substitution box (S-box) when encrypting the other portion.

2. (Original) One or more computer readable-media as recited in claim 1, wherein the entire digital good is to be encrypted.

3. (Original) One or more computer readable media as recited in claim 1, wherein the using comprises determining, for each group of bits of the other portion, a new group of bits based on the portion.

4. (Original) One or more computer readable media as recited in claim 1, wherein the using comprises using bits of the portion to determine a substitution sub-portion for each sub-portion in the other portion.

5. (Original) One or more computer readable media as recited in claim 4, wherein the sub-portion comprises a byte.

6. (Original) One or more computer readable media as recited in claim 1, wherein the digital good comprises a software program.

7. (Original) One or more computer readable media as recited in claim 1, wherein the digital good includes video content.

8. (Previously presented) A method comprising:
selecting a segment of a digital good;
selecting another segment of the digital good, wherein the other segment is to be encrypted using an encryption process; and
mapping, as at least part of the encryption process, values within the other segment to new values based on the segment, wherein the mapping comprises using the segment as a substitution box (S-box) during the encryption process.

9. (Original) A method as recited in claim 8, wherein the entire digital good is to be encrypted by the encryption process.

10. (Canceled).

11. (Original) A method as recited in claim 8, wherein the mapping comprises determining, for each group of bits of the other segment, a new group of bits based on the segment.

12. (Original) A method as recited in claim 8, wherein the mapping comprises using bits of the segment to determine a new value for each value in the other segment.

13. (Original) A method as recited in claim 8, wherein the digital good comprises a software program.

14. (Original) A method as recited in claim 8, wherein the digital good includes video content.

15. (Original) A method as recited in claim 8, wherein the encryption process uses a Data Encryption Standard (DES) cipher.

16. (Original). One or more computer-readable memories comprising computer-readable instructions that, when executed by a processor, direct a computer system to perform the method as recited in claim 8.

17. (Original) A method comprising:
using at least a portion of a digital good as a substitution box (S-box).

18. (Original) A method as recited in claim 17, wherein the using comprises using the portion of the digital good as a substitution box to encrypt another portion of the digital good.

19. (Original) A method as recited in claim 18, wherein the using comprises determining, for each group of bits of the other portion, a new group of bits based on the portion.

20. (Original) A method as recited in claim 18, wherein the using comprises using a bit pattern of the portion to determine a substitution value for each value in the other portion.

21. (Original) A method as recited in claim 17, wherein the digital good comprises a software program.

22. (Original) A method as recited in claim 17, wherein the digital good includes video content.

23. (Original) A method as recited in claim 17, wherein the using comprises using the substitution box as part of a Data Encryption Standard (DES) cipher.

24. (Original) One or more computer-readable memories comprising computer-readable instructions that, when executed by a processor, direct a computer system to perform the method as recited in claim 17.

25. (Original) A production system, comprising:
a memory to store an original program; and

a production server equipped with a substitution box (S-box) protection tool that is used to augment the original program for protection purposes, the production server being configured to identify a first segment in the original program and use the first segment as an S-box when encrypting a second segment of the original program.

26. (Original) A production system as recited in claim 25, wherein the production server is further configured to use the first segment as an S-box by determining, for each group of bits of the second segment, a new group of bits based on the first segment.

27. (Original) A production system as recited in claim 25, wherein the production server is further configured to use the first segment as an S-box by using bits of the first segment to determine a substitution value for each value in the second segment.

28. (Original) A production system as recited in claim 25, wherein the production server is to encrypt the entire digital good.

29. (Original) A production system as recited in claim 25, wherein the digital good includes one or more of: a software program, audio content, and video content.

30. (Original) A production system as recited in claim 25, wherein the production server uses a Data Encryption Standard (DES) cipher to encrypt the second segment.

31. (Original) A client-server system, comprising:
a production server to use a portion of a first digital good as a substitution box (S-box) in encrypting at least a portion of a second digital good to produce a protected digital good; and

a client to store and execute the protected digital good, the client being configured to evaluate the protected digital good to determine whether the protected digital good has been tampered with.

32. (Original) A client-server system as recited in claim 31, wherein the first digital good and the second digital good are the same digital good.

33. (Original) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors, causes the one or more processors to perform acts including:

decrypting at least a portion of a digital good by using another portion of the digital good as a substitution box (S-box).

34. (Original) One or more computer readable media as recited in claim 33, wherein the decrypting is based at least in part on a Data Encryption Standard (DES) cipher.

35. (Original) One or more computer readable media as recited in claim 33, wherein the decrypting comprises using bits of the other portion to determine a substitution value for each value in the portion.

36. (Original) One or more computer readable media as recited in claim 33, wherein the digital good includes one or more of: a software program, audio content, and video content.

(9) Appendix of Evidence Submitted

None.

(10) Appendix of Related Proceedings

None.